IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION AT COLUMBUS

Mohammad S. Galaria, individually and on behalf of all others similarly situated, Plaintiff, v. Nationwide Mutual Insurance Company, an Ohio Corporation, Defendant.	Case No. 2:13-cv-118 Judge **CLASS ACTION COMPLAINT**

Plaintiff Mohammad S. Galaria ("Plaintiff"), individually and on behalf of all others similarly situated, complains of the actions of defendant Nationwide Mutual Insurance Company ("Nationwide" or "Defendant"), and respectfully alleges the following:

NATURE OF THE CASE

1. This is a consumer class action brought by Plaintiff, individually and on behalf of all others similarly situated (*i.e.*, the Class Members), seeking to redress Defendant's intentional, willful and reckless violations of their privacy rights. Plaintiff and the other Class Members are consumers of insurance coverage who entrusted their personally identifiable information ("PII") to Defendant. Defendant betrayed Plaintiff's trust by failing to properly safeguard and protect their PII and publicly disclosing their PII without authorization in violation of numerous laws, including, *inter alia*, the Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.* ("FCRA"), and applicable common law.

2. This action pertains to a October 3, 2012, unauthorized intrusion into a portion of Nationwide's computer network used by Nationwide and Allied Insurance

Company, an affiliate of Nationwide (the "Data Breach"), during which Plaintiff's and the other Class Members' PII was stolen and disseminated to unauthorized persons as a direct and/or proximate result of Defendant's failure to safeguard and protect their PII. The wrongfully disclosed PII included, *inter alia*, Plaintiff's and the other Class Members' names, and some combination of their Social Security numbers, driver's license numbers, dates of birth, marital statuses, genders, occupations, and their employers' names and addresses.

3. Defendant flagrantly disregarded Plaintiff's and the other Class Members' privacy and property rights by intentionally, willfully and recklessly failing to take the necessary precautions required to safeguard and protect Plaintiff's and the other Class Members' PII from unauthorized disclosure. Plaintiff's and the other Class Members' PII was improperly handled, inadequately protected, readily able to be copied by data thieves and not kept in accordance with basic security protocols. Defendant's obtaining of the information and sharing of same also represent a flagrant disregard of Plaintiff's and the other Class Members' rights, both as to privacy and property.

4. Plaintiff has standing to bring this action because as a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Data Breach, Plaintiff has incurred (and will continue to incur) damages in the form of, *inter alia*, (i) loss of privacy and/or (ii) the additional damages set forth in detail below, which are incorporated herein by reference.

5. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Data Breach, Plaintiff and the other Class Members have been deprived of the value of their PII, for which there is a well-established national and international market. For example, stolen PII is sold on the cyber black

market for $14 to $25 per record to (i) individuals needing or wanting a new identity or healthcare, or focused on committing fraud, (ii) medical service providers, medical device manufacturers and drug manufacturers for targeted marketing and advertising campaigns for their products and services, and (iii) health insurers for targeted marketing and advertising campaigns for their health insurance products and to monitor their insureds' medical conditions for purposes of adjusting their health insurance premiums.

6. Defendant's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiff and the other Class Members at an imminent, immediate and continuing increased risk of identity theft, identity fraud and medical fraud. Indeed, Javelin Strategy & Research ("Javelin"), a leading provider of quantitative and qualitative research, recently released its 2012 Identity Fraud Report ("the Javelin Report"), quantifying the impact of data breaches. According to the Javelin Report, individuals whose PII is subject to a reported data breach—such as the Data Breach at issue here—are approximately 9.5 times more likely than the general public to suffer identity fraud and/or identity theft. Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported, and a high probability that criminals who may now possess Plaintiff's and the other Class Members' PII and not yet used the information will do so at a later date or re-sell it.

7. Accordingly, Plaintiff and the other Class Members seek redress against Defendant for, *inter alia*, violations of the FCRA, invasion of privacy by the public disclosure of private facts, common law negligence and bailment.

8. Plaintiff, on behalf of himself and the other Class Members, seeks (i) actual damages, economic damages, statutory damages under FCRA, and/or nominal damages, (ii) exemplary damages, (iii) injunctive relief, and (iv) attorneys' fees, litigation expenses, and costs.

JURISDICTION AND VENUE

9. The Court has subject matter jurisdiction over Plaintiff's FCRA claims pursuant to (i) 28 U.S.C. § 1331 (federal question), and (ii) 28 U.S.C. § 1332(d) ("CAFA") because (a) there are 100 or more Class Members, (b) at least one Class Member is a citizen of a state that is diverse from Defendant's citizenship, and (c) the matter in controversy exceeds $5,000,000 USD exclusive of interest and costs. The Court also has subject matter jurisdiction over Plaintiff's state law claims pursuant to 28 U.S.C. § 1367. The Court has personal jurisdiction over Defendant because at all relevant times, Defendant was and is an Ohio corporation with its principal place of business in Columbus, Ohio, that conducted (and continues to conduct) substantial business in the Ohio.

10. Venue is proper in this District pursuant to 28 U.S.C. §1391(b) because Defendant is an Ohio corporation with its principal place of business in Columbus, Ohio, it conducts substantial business in this District, and a substantial part of the events or omissions giving rise to the claims occurred in this District.

PARTIES

11. Plaintiff is a citizen and resident of Mower County, Minnesota. Defendant possessed Plaintiff's sensitive personal information (*i.e.*, his PII), which Defendant was required to safeguard and properly protect, as well as lawfully obtain and retain.

Plaintiff received a November 16, 2012 letter from Defendant, as did the other Class Members at or about the same time, informing him about the Data Breach and the fact that his PII was stolen, disseminated without authorization and compromised. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Data Breach, Plaintiff has suffered the economic damages and other actual harm set forth above. Defendant's wrongful disclosure of Plaintiff's PII has also placed him at an imminent, immediate and continuing increased risk of harm for identity theft, identity fraud and medical fraud.

12. Defendant Nationwide is an Ohio corporation with its principal place of business in Columbus, Ohio. Nationwide is "one of the largest insurance and financial services companies in the world, with more than $135 billion in statutory assets." *See* http://www.nationwide.com/about-us/history.jsp (last visited Feb. 8, 2013). At all relevant times, Defendant was (and continues to be) entrusted with, and obligated to safeguard and protect Plaintiff's and the other Class Members' PII in connection with the insurance products purchased and/or sought to be purchased by Plaintiff and the other Class Members in consumer transactions during the Class Period—to-wit, in order to purchase and/or seek to purchase insurance products sold by Defendant, Plaintiff and the other Class Members were required to provide or have provided their PII to Defendant. Defendant is also a Consumer Reporting Agency as defined under the FCRA because it regularly engages, in whole or in part, in the practice of assembling information on consumers for the purpose of furnishing consumer reports to third parties and/or uses interstate commerce for the purpose of preparing and/or furnishing consumer reports, within the meaning of the FCRA, 15 U.S.C. § 1681 *et seq.*

BACKGROUND FACTS

13. Nationwide collects PII from consumers and other sources in order to provide quotes and sales to consumers for its insurance products and services. *See* http://www. nationwide.com/notice-faq.jsp (last visited on Feb. 8, 2013). Plaintiff purchased a Nationwide insurance policy. Nationwide has wrongfully retained and failed to safeguard and protect Plaintiff's and the other Class Members' PII.

14. On October 3, 2012, a portion of Nationwide's computer network, which is used by Nationwide and its insurance agents and Allied Insurance Company ("Allied") and its insurance agents, was intruded upon by an unauthorized person(s), resulting in the theft and wrongful dissemination of Plaintiff's and the other Class Members' PII (*i.e.*, the Data Breach). Nationwide reported that the Data Breach affected an estimated 1.1 million customers and non-customers who had purchased insurance products from Nationwide or sought insurance quotations.

15. As a direct and/or proximate result of Defendant's failure to properly safeguard and protect the PII of its customers and non-customers, Plaintiff's and the other Class Members' PII was stolen, wrongfully disseminated without authorization and compromised.

16. More than six weeks after the Data Breach occurred, Plaintiff received a November 16, 2012 letter from Nationwide informing him of the Data Breach and the fact that his PII had been wrongfully disseminated without authorization and compromised. On information and belief, Nationwide sent the uniform letter to all other Class Members.

17. Nationwide's letter encouraged Plaintiff to take certain steps to protect his PII against misuse, advised him to be vigilant and suggested that he closely monitor his bank statements, credit reports and other financial information for unusual activity. *Id.*

Nationwide offered Plaintiff only one year of free credit monitoring and identity theft protection through Equifax, which provides under certain conditions up to $1 million identity fraud expense coverage and access to his credit report. Nationwide also provided directions to Plaintiff and the other Class Members for placing a fraud alert.

18. Nationwide also suggested and directed that Plaintiff and the other Class members could place a security freeze on their credit reports, which Nationwide states is "intended to prevent credit, loans and services from being approved in [an individual's] name without [that individual's] consent; however, using a security freeze may delay your ability to obtain credit." *See* http://www.nationwide.com/notice-resources.jsp (last visited Feb. 8, 2013). Nationwide, however, did not offer to pay this expense. Further, according to Nationwide, as stated on the referenced webpage, a credit bureau "may charge a fee of up to $5.00 (and in some cases, up to $20.00) to place a freeze or lift or remove a freeze." *Id.*

19. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Data Breach, the criminal(s) and/or their customers now have Plaintiff's and the other Class Members' compromised PII. There is a robust international market for the purloined PII. Defendant's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiff and the other Class Members at an imminent, immediate and continuing increased risk of identity theft, identity fraud[1] and medical fraud.

[1]According to the United States Government Accounting Office (GAO), the terms "identity theft" or "identity fraud" are broad terms encompassing various types of criminal activities. Identity theft occurs when PII is used to commit fraud or other crimes. These crimes include, *inter alia*, credit card fraud, phone or utilities fraud, bank fraud and government fraud (theft of government services).

20. Identity theft occurs when someone uses an individual's PII, such as the person's name, Social Security number, or credit card number, without the individual's permission, to commit fraud or other crimes. *See* http://www.consumer.ftc.gov/articles/pdf-0014-identity-theft.pdf (last visited Feb. 8, 2013).

21. The Federal Trade Commission correctly sets forth that "Identity theft is a serious crime. It can disrupt your finances, credit history, and reputation, and take time, money, and patience to resolve." *Id.*

22. Identity theft crimes often involve more than just crimes of financial loss, such as various types of government fraud (such as obtaining a driver's license or official identification card in the victim's name but with their picture), using a victim's name and Social Security number to obtain government benefits and/or filing a fraudulent tax return using a victim's information. Identity thieves also obtain jobs using stolen Social Security numbers, rent houses and apartments and/or obtain medical services in a victim's name. Identity thieves also have been known to give a victim's PII to police during an arrest, resulting in the issuance of an arrest warrant in the victim's name and an unwarranted criminal record.

23. According to the FTC, "the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and that any privacy framework should recognize additional harms that might arise from unanticipated uses of data."[2] Furthermore, "there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead

[2]*Protecting Consumer Privacy in an Era of Rapid Change* FTC, Report March 2012 (http://www.ftc.gov/os/ 2012/03/120326privacyreport.pdf).

to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII."[3]

24. According to the Javelin Report, in 2011, the mean consumer cost of rectifying identity fraud was $354 while the mean resolution time of identity fraud was 12 hours. *Id.* at 6. In 2011, the consumer cost for new account fraud and existing non-card fraud increased 33% and 50% respectively. *Id.* at 9. Consumers who received a data breach notification had a fraud incidence rate of 19% in 2011 and, of those experiencing fraud, 43% reported their credit card numbers were stolen and 22% of the victims reported their debit card numbers were stolen. *Id.* at 10. More important, consumers who were notified that their PII had been breached were 9.5 times more likely to experience identity fraud than consumers who did not receive such a notification. *Id.* at 39.

25. The unauthorized disclosure of a person's Social Security number can be particularly damaging since Social Security numbers cannot be easily replaced like a credit card or debit card. In order to obtain a new Social Security number, a person must show evidence that someone is using the number fraudulently or is being disadvantaged by the misuse. *See* Identity Theft and Your Social Security Number, SSA Publication No. 05-10064, October 2007, ICN 46327 (http://www.ssa.gov/pubs/10064.html) (last accessed Feb. 8, 2013). Thus, a person whose PII has been stolen cannot obtain a new Social Security number until the damage has already been done.

---

[3]*Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report*, 35-38 (Dec. 2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf; *Comment of Center for Democracy & Technology*, cmt. #00469, at 3; *Comment of Statz, Inc.*, cmt. #00377, at 11-12.

26. Obtaining a new Social Security number also is not an absolute prevention against identity theft. Government agencies, private businesses and credit reporting companies likely still have the person's records under the old number, so using a new number will not guarantee a fresh start. For some victims of identity theft, a new number may actually create new problems; because prior positive credit information is not associated with the new Social Security number, it is more difficult to obtain credit due to the absence of a credit history.

27. Medical fraud (or medical identity theft) occurs when a person's personal information is used without authorization to obtain, or receive payment for, medical treatment, services or goods. For example, as of 2010, more than 50 million people in the United States did not have health insurance according to the U.S. census. This, in turn, has led to a surge in medical identity theft as a means of fraudulently obtaining medical care. Victims of medical identity theft also may find that their medical records are inaccurate, which can have a serious impact on their ability to obtain proper medical care and insurance benefits.

28. The Data Breach and Defendant's untimely and inadequate notification of the Data Breach also substantially increased Plaintiff's and the other Class Members' risk of being victimized by "phishing." "Phishing" is an attempt to acquire information (and sometimes, indirectly, money), such as usernames, passwords and credit card details by masquerading as a trustworthy entity through an electronic communication. *See* http://www.onguardonline.gov/articles/0003-phishing (last visited Feb. 8, 2013). Communications purporting to be from popular social websites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public. Phishing emails may contain links to websites that are

infected with malware. Phishing is typically carried out by e-mail spoofing or instant messaging, and often directs users to enter details at a fake website that looks and feels almost identical to the legitimate one. When criminals have access to PII from a large group of similarly situated victims, it is much more feasible to develop a believable phishing spoof email. They can then get this group of victims to reveal additional private information, such as credit cards, bank accounts, and the like.

29. Defendant flagrantly disregarded and/or violated Plaintiff's and the other Class Members' privacy and property rights, and harmed them in the process, by not obtaining Plaintiff's and the other Class Members' prior written consent to disclose their PII to any other person—as required by FCRA and other pertinent laws, regulations, industry standards and/or internal company standards.

30. Defendant flagrantly disregarded and/or violated Plaintiff's and the other Class Members' privacy and property rights, and harmed them in the process, by failing to safeguard and protect and, in fact, wrongfully disseminating Plaintiff's and the other Class Members' PII to unauthorized persons.

31. Defendant flagrantly disregarded and/or violated Plaintiff's and the other Class Members' privacy and property rights, and harmed them in the process, by failing to keep or maintain an accurate accounting of the PII wrongfully disclosed in the Data Breach, as made evident by, *inter alia*, Nationwide's admission that it is "still investigating the incident" and that "[a]t this time" it does not think that "any medical information or credit card account information was stolen in the attack." *See* http://www.nationwide.com/notice.jsp (last visited Feb. 8, 2013).

32. Defendant flagrantly disregarded and/or violated Plaintiff's and the other Class Members' privacy rights, and harmed them in the process, by failing to establish

and/or implement appropriate administrative, technical and/or physical safeguards to ensure the security and confidentiality of Plaintiff's and the other Class Members' PII to protect against anticipated threats to the security or integrity of such information. Defendant's unwillingness or inability to establish and maintain the proper information security procedures and controls is an abuse of discretion and confirms its intentional and willful failure to observe procedures required by law, industry standards and/or their own internal policies and procedures.

33. Defendant flagrantly disregarded and/or violated Plaintiff's and the other Class Members' privacy rights, and harmed them in the process, by depriving Plaintiff and the other Class Members of the value of their PII, for which there is a well-established national and international market. *See, e.g.*, T. Soma, *et al*, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

34. Aside from the criminal element, frequent purchasers of purloined PII include other data thieves and fraudsters, pharmacies, drug manufacturers, medical device manufacturers, hospitals and insurance companies, who use the information to market their products and services directly to the data breach victims and/or to adjust the victims' medical insurance premiums. Plaintiff and the other Class Members, not data thieves, should have the right to sell their PII and receive the corresponding financial benefits.

35. The actual harm and adverse effects to Plaintiff and the other Class Members, including the imminent, immediate and continuing increased risk of harm for

identity theft, identity fraud and/or medical fraud directly and/or proximately caused by Defendant's above wrongful actions and/or inaction and the resulting Data Breach requires Plaintiff and the other Class Members to take affirmative acts to recover their peace of mind, and personal security including, without limitation, purchasing credit reporting services, purchasing credit monitoring and/or internet monitoring services, frequently obtaining, purchasing and reviewing credit reports, bank statements, and other similar information, instituting and/or removing credit freezes and/or closing or modifying financial accounts—for which there is a financial and temporal cost. Plaintiff and the other Class Members have suffered, and will continue to suffer, such damages for the foreseeable future.

36. Victims and potential victims of identity theft, identity fraud and/or medical fraud—such as Plaintiff and the other Class Members—typically spend hundreds of hours in personal time and hundreds of dollars in personal funds to resolve credit and other financial issues resulting from data breaches. According to the Javelin Report, not only is there a substantially increased risk of identity theft and identity fraud for data breach victims, those who are further victimized by identity theft or identity fraud will incur an average fraud-related economic loss of $1,513 and incur an average of $354 of out-of-pocket expenses attempting to rectify the situation. *Id*. at 6.

37. Other statistical analyses are in accord. The GAO found that identity thieves use PII to open financial accounts and payment card accounts and incur charges in a victim's name. This type of identity theft is the "most damaging" because it may take some time for the victim to become aware of the theft, in the meantime causing significant harm to the victim's credit rating and finances. Moreover, unlike other PII, Social Security numbers are incredibly difficult to change and their misuse can continue

for years into the future. The GAO states that victims of identity theft face "substantial costs and inconvenience repairing damage to their credit records," as well the damage to their "good name."

38. Defendant's wrongful actions and/or inaction directly and/or proximately caused the theft and dissemination into the public domain of Plaintiff's and the other Class Members' PII without their knowledge, authorization and/or consent. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Data Breach, Plaintiff and the other Class Members have incurred (and will continue to incur) damages in the form of, *inter alia*, (i) loss of privacy, (ii) the imminent, immediate and continuing increased risk of identity theft, identity fraud and/or medical fraud, (iii) out-of-pocket expenses to purchase credit monitoring, internet monitoring, identity theft insurance and/or other Data Breach risk mitigation products, (iv) out-of-pocket expenses incurred to mitigate the increased risk of identity theft, identity fraud and/or medical fraud pressed upon them by the Data Breach, including the costs of placing a credit freeze and subsequently removing a credit freeze, (v) the value of their time spent mitigating the increased risk of identity theft, identity fraud and/or medical fraud pressed upon them by the Data Breach, and/or (vi) deprivation of the value of their PII/PHI, for which there is a well-established national and international market.

CLASS ACTION ALLEGATIONS

39. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings this class action as a national class action on behalf of himself and the following Class of similarly situated individuals:

> All persons who sought an insurance quote from Nationwide Mutual Insurance Company or Allied Insurance Company, and whose names, and some combination of their Social Security numbers, driver's license numbers, dates of birth, marital statuses, genders, occupations, and their employers' names and addresses, were compromised by the October 3, 2012 data breach of the computer network used by Nationwide Mutual Insurance Company and Allied Insurance Company agents. The Class specifically excludes Defendant, any entity in which Defendant has a controlling interest, Defendant's officers, directors, agents and/or employees, the Court and Court personnel.

40. On information and belief, the putative Class is comprised of approximately 1.1 million geographically dispersed people, making joinder impracticable. Disposition of this matter as a class action will provide substantial benefits and efficiencies to the Parties and the Court.

41. The rights of Plaintiff and each other Class Member were violated in a virtually identical manner as a direct and/or proximate result of Defendant's willful, reckless and/or negligent actions and/or inaction and the resulting Data Breach.

42. Questions of law and fact common to all Class Members exist and predominate over any questions affecting only individual Class Members including, *inter alia*:

a) Whether Defendant violated FCRA by failing to properly obtain, maintain, secure or protect Plaintiff's and the other Class Members' PII;

b) Whether Defendant willfully, recklessly and/or negligently failed to maintain and/or execute reasonable procedures designed to prevent unauthorized access to Plaintiff's and the other Class Members' PII;

c) Whether Defendant was negligent in failing to properly safeguard and protect Plaintiff's and the other Class Members' PII;

d) Whether Defendant owed a duty to Plaintiff and the other Class Members to exercise reasonable care in safeguarding and protecting their PII;

e) Whether Defendant breached its duty to exercise reasonable care in failing to safeguard and protect Plaintiff's and the other Class Members' PII;

f) Whether Defendant was negligent in failing to safeguard and protect Plaintiff's and the other Class Members' PII;

g) Whether, by publicly disclosing Plaintiff's and the other Class Members' PII without authorization, Defendant invaded their privacy; and

h) Whether Plaintiff and the other Class Members sustained damages as a result of Defendant's failure to safeguard and protect their PII.

43. Plaintiff and his counsel will fairly and adequately represent the interests of the other Class Members. Plaintiff has no interests antagonistic to, or in conflict with, the other Class Members' interests. Plaintiff's lawyers are highly experienced in the prosecution of consumer class action and data breach cases.

44. Plaintiff's claims are typical of the other Class Members' claims in that Plaintiff's claims and the other Class Members' claims all arise from Defendant's failure to properly safeguard and protect their PII.

45. A class action is superior to all other available methods for fairly and efficiently adjudicating Plaintiff's and the other Class Members' claims. Plaintiff and the other Class Members have been harmed as a result of Defendant's wrongful actions and/or inaction and the resulting Data Breach. Litigating this case as a class action will reduce the possibility of repetitious litigation relating to Defendant's conduct.

46. Class certification, therefore, is appropriate pursuant to FED. R. CIV. P. 23(b)(3) because the above common questions of law or fact predominate over any

questions affecting individual Class Members, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

47. Class certification also is appropriate pursuant to FED. R. CIV. P. 23(b)(2) because Defendant has acted or refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

48. The expense and burden of litigation would substantially impair the ability of Class Members to pursue individual lawsuits in order to vindicate their rights. Absent a class action, Defendant will retain the benefits of its wrongdoing despite its serious violations of the law.

CLAIMS FOR RELIEF/CAUSES OF ACTION

COUNT I

WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT

49. The preceding factual statements and allegations are incorporated herein by reference.

50. FCRA requires consumer reporting agencies to adopt and maintain procedures for meeting the needs of commerce for consumer credit, personnel, insurance and other information in a manner fair and equitable to consumers while maintaining the confidentiality, accuracy, relevancy and proper utilization of such information. 15 U.S.C. § 1681(b).

51. FCRA defines a "consumer reporting agency" as:

> Any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of

> interstate commerce for the purpose of preparing or furnishing consumer reports.

15 U.S.C. § 1681a(f).

52. FCRA defines a "consumer report" as:

> [A]ny written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of establishing the consumer's eligibility for credit or insurance to be used primarily for personal, family, or household purposes; employment purposes, or any other purpose authorized under [15 U.S.C. §] 1681(b).

15 U.S.C. § 1681a(d)(1).

53. Defendant is a Consumer Reporting Agency as defined under FCRA because on a cooperative nonprofit basis and/or for monetary fees, Defendant regularly engages, in whole or in part, in the practice of assembling Plaintiff's and the other Class Members' PII for the purpose of furnishing Consumer Reports to third parties in connection with providing insurance quotes and/or uses interstate commerce for the purpose of preparing and/or furnishing Consumer Reports in connection with providing insurance quotes.

54. Plaintiff's and the other Class Members' PII constitute Consumer Reports because they bear on, *inter alia*, their credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, physical/medical conditions, and mode of living, which is used or collected, in whole or in part, for the purpose of establishing Plaintiff's and the other Class Members' eligibility for insurance to be used primarily for personal, family, or household purposes.

55. As a Consumer Reporting Agency, Defendant was (and continues to be) required to adopt and maintain procedures designed to protect and limit the dissemination of consumer credit, personnel, insurance and other information in a manner fair and equitable to consumers while maintaining the confidentiality, accuracy, relevancy, and proper utilization of such information. Defendant, however, violated FCRA by failing to adopt and maintain such protective procedures which, in turn, directly and/or proximately resulted in the theft and wrongful dissemination of Plaintiff's and the other Class Members' PII into the public domain.

56. Defendant's violation of FCRA, as set forth above, was willful or, at the very least, reckless, constituting willfulness.

57. As a direct and/or proximate result of Defendant's willful and/or reckless violations of FCRA, as described above, Plaintiff's and the other Class Members' PII was stolen, made accessible to unauthorized third parties in the public domain and compromised.

58. As a further direct and/or proximate result of Defendant's willful and/or reckless violations of FCRA, as described above, Plaintiff and the other Class Members were (and continue to be) injured and have suffered (and will continue to suffer) the damages described in detail above. Defendant's wrongful actions and/or inaction violated FCRA.

59. Plaintiff and the other Class Members, therefore, are entitled to compensation for their actual damages including, *inter alia*, expenses for adequate credit monitoring and identity theft insurance, out-of-pocket expenses, such as costs for placing a credit freeze or removing a credit freeze, loss of privacy, deprivation of the value of their PII, and other economic and non-economic harm (as detailed above), or

statutory damages of not less than $100, and not more than $1,000, each, as well as attorneys' fees, litigation expenses and costs, pursuant to 15 U.S.C. § 1681n(a).

COUNT II

NEGLIGENT VIOLATION OF THE FAIR CREDIT REPORTING ACT

60. The preceding factual statements and allegations are incorporated herein by reference.

61. Defendant owed a duty to Plaintiff and the other Class Members to safeguard and protect their PII. In the alternative, and as described above, Defendant negligently violated FCRA by failing to adopt and maintain procedures designed to protect and limit the dissemination of Plaintiff's and the other Class Members' PII for the permissible purposes outlined by FCRA which, in turn, directly and/or proximately resulted in the theft and wrongful dissemination of Plaintiff's and the other Class Members' PII into the public domain.

62. It was reasonably foreseeable that Defendant's failure to maintain procedures to safeguard and protect Plaintiff's and the other Class Members' PII would result in an unauthorized third party gaining access to their PII for no permissible purpose under FCRA.

63. As a direct and/or proximate result of Defendant's negligent violations of FCRA, as described above, Plaintiff's and the other Class Members' PII was stolen, made accessible to unauthorized third parties in the public domain and compromised.

64. As a further direct and/or proximate result of Defendant's willful and/or reckless violations of FCRA, as described above, Plaintiff and the other Class Members

were (and continue to be) injured and have suffered (and will continue to suffer) the damages described in detail above. Defendant's wrongful actions and/or inaction violated FCRA.

65. Plaintiff and the other Class Members, therefore, are entitled to compensation for their actual damages, including, *inter alia*, expenses for adequate credit monitoring and identity theft insurance, out-of-pocket expenses, such as costs for placing a credit freeze or removing a credit freeze, loss of privacy, deprivation of the value of their PII, and other economic and non-economic harm (as detailed above), as well as attorneys' fees, litigation expenses and costs, pursuant to 15 U.S.C. §1681o(a).

COUNT III

NEGLIGENCE

66. The preceding factual statements and allegations are incorporated herein by reference.

67. Defendant owed a duty to Plaintiff and the other Class Members to safeguard and protect their PII.

68. Defendant breached its duty by failing to exercise reasonable care and failing to safeguard and protect Plaintiff's and the other Class Members' PII.

69. It was reasonably foreseeable that Defendant's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the other Class Members' PII would result in an unauthorized third party gaining access to such information for no lawful purpose.

70. Plaintiff and the other Class Members were (and continue to be) damaged as a direct and/or proximate result of Defendant's failure to secure and protect their PII in the form of, *inter alia*, expenses for adequate credit monitoring and identity theft

insurance, out-of-pocket expenses, such as costs for placing a credit freeze or removing a credit freeze, loss of privacy, deprivation of the value of their PII, and other economic and non-economic harm (as detailed above), for which they are entitled to compensation.

71. Defendant's wrongful actions and/or inaction and the resulting Data Breach (as described above) constituted (and continue to constitute) negligence at common law.

COUNT IV

INVASION OF PRIVACY BY PUBLIC DISCLOSURE OF PRIVATE FACTS

72. The preceding factual statements and allegations are incorporated herein by reference.

73. Plaintiff's and the other Class Members' PII was (and continues to be) sensitive and personal private information.

74. By virtue of Defendant's failure to safeguard and protect Plaintiff's and the other Class Members' PII and the resulting Data Breach, Defendant wrongfully disseminated Plaintiff's and the other Class Members' PII to unauthorized persons.

75. Dissemination of Plaintiff's and the other Class Members' PII is not of a legitimate public concern; publicity of their PII was, is and will continue to be offensive to Plaintiff, the other Class Members and all reasonable people. The unlawful disclosure of same violates public mores.

76. Plaintiff and the other Class Members were (and continue to be) damaged as a direct and/or proximate result of Defendant's invasion of their privacy by publicly

disclosing their private facts (*i.e.*, their PII) in the form of, *inter alia*, expenses for adequate credit monitoring and identity theft insurance, out-of-pocket expenses, such as costs for placing a credit freeze or removing a credit freeze, loss of privacy, deprivation of the value of their PII, and other economic and non-economic harm (as detailed above), for which they are entitled to compensation. At the very least, Plaintiff and the other Class Members are entitled to nominal damages.

77. Defendant's wrongful actions and/or inaction and the resulting Data Breach (as described above) constituted (and continue to constitute) an invasion of Plaintiff's and the other Class Members' privacy by publicly and wrongfully disclosing their private facts (*i.e.*, their PII) without their authorization or consent.

COUNT V

BAILMENT

78. The preceding factual statements and allegations are incorporated herein by reference.

79. Plaintiff and the other Class Members entrusted their PII to Defendant and/or its affiliate, Allied, for the purpose of obtaining insurance quotes for insurance products and services offered by Nationwide and/or Allied, or to others for similar purposes. Plaintiff and the other Class Members were entitled to trust that their PII in Nationwide's or Allied's possession would likewise be properly protected from unlawful access whether or not they originally entrusted it to Nationwide.

80. Plaintiff's and the other Class Members' PII is their personal property. Defendant's wrongful actions and/or inaction and the resulting Data Breach deprived them of the value of their PII, for which there is a well-established national and

international market, because the PII is now in the hands of unauthorized person(s) and compromised.

81. Further, Defendant wrongfully retained and failed to safeguard and protect the PII of Plaintiff and the other Class Members.

82. During the time of bailment, Defendant owed Plaintiff and the other Class Members the duty to safeguard and protect their PII by maintaining reasonable and effective data security practices, procedures and protocols to protect their PII. As alleged herein, Defendant breached its duty to Plaintiff and the other Class Members by failing to safeguard and protect their PII which, in turn, directly and/or proximately caused the Data Breach and the wrongful dissemination of their PII to unauthorized persons.

83. Defendant's breach of this duty directly and/or proximately caused Plaintiff and the other Class Members to suffer (and continue to suffer) the injuries and damages alleged herein.

RELIEF REQUESTED

84. The preceding factual statements and allegations are incorporated herein by reference.

85. **DAMAGES.** As a direct and/or proximate result of Defendant's wrongful actions and/or inaction (as described above) and the resulting Data Breach, Plaintiff and the other Class Members have damages in the form of, *inter alia*, loss of time to closely monitor their credit card and debit card transactions and address any unauthorized charges, expenses for adequate credit monitoring and identity theft insurance, out-of-pocket expenses, such as costs for placing a credit freeze or removing a credit freeze, loss of privacy, deprivation of the value of their PII and other economic and non-economic

harm, for which they are entitled to compensation. Plaintiff and the other Class Members also are entitled to recover statutory damages and/or nominal damages. Plaintiff's and the other Class Members' damages were foreseeable by Defendant and exceed the minimum jurisdictional limits of the Court.

86. **EXEMPLARY DAMAGES.** Plaintiff and the other Class Members also are entitled to exemplary damages as punishment and to deter such wrongful conduct in the future.

87. **INJUNCTIVE RELIEF.** Plaintiff and the other Class Members also are entitled to injunctive relief mandating, *inter alia*, (i) adequate credit monitoring, *i.e.*, more than one year; (ii) adequate identity theft insurance, *i.e.*, more than one year; (iii) identity theft remediation services; (iv) coverage for all costs, losses and expenses resulting from the Data Breach, including lost time and wages; (v) a correct and complete statement to each Class Member as to the nature of the information of that Class Member that was breached; (vi) notification to each Class Member that they may have his or her information removed from the database; (vii) an order requiring Nationwide to advise each person whose information that it chooses to maintain that it intends on doing so and that it will not do so until it has received permission from the consumer to do so; and (viii) Defendant to submit to periodic data security compliance audits for a period of twenty years by a third party regarding the security of consumers' PII in its possession, custody and control.

88. **ATTORNEYS' FEES, LITIGATION EXPENSES, AND COSTS.** Plaintiff and the other Class Members also are entitled to recover their attorneys' fees, litigation expenses and court costs in prosecuting this action pursuant to, *inter alia*, 15 U.S.C. §§ 1681n(a), o(a).

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, respectfully requests that (i) this action be certified as a class action; (ii) Plaintiff be designated the Class Representative; and (iii) Plaintiff's counsel be appointed as Class Counsel. Plaintiff, on behalf of himself and the other Class Members, further requests that upon final trial or hearing, judgment be awarded against Defendant, in favor of Plaintiff and the other Class Members, for:

(i) actual damages, consequential damages, FCRA statutory damages and/or nominal damages (as described above) in an amount to be determined by the trier of fact;

(ii) exemplary damages:

(iii) injunctive relief, as set forth above;

(iv) pre- and post-judgment interest at the highest applicable legal rates;

(v) attorneys' fees and litigation expenses incurred through trial and any appeals;

(iv) costs of suit; and

(vi) such other and further relief that this Court deems just and proper.

JURY DEMAND

Plaintiff, on behalf of himself and the other Class Members, respectfully demands a trial by jury on all of his claims and causes of action so triable.

Respectfully submitted,

/s/ Charles T. Lester, Jr.

Charles T. Lester, Jr. (0017601)
Attorney for Plaintiff
P.O. Box 75069
Fort Thomas, KY 41075-0069
(859) 838-4294, (859) 781-2406
Fax: (859) 486-6590
Email: cteljr@fuse.net, cteljr@yahoo.com

OF COUNSEL:

Ben Barnow
BARNOW AND ASSOCIATES, P.C.
One N. LaSalle Street, Ste. 4600
Chicago, IL 60602
Telephone: (312) 621-2000
Facsimile: (312) 641-5504
Email: b.barnow@barnowlaw.com

Ralph K. Phalen
RALPH K. PHALEN LAW, P.C.
1000 Broadway, Suite 400
Kansas City, MO 6410
Telephone: (816) 589-0753
Facsimile: (816) 471-1701
Email: phalenlaw@yahoo.com

Richard L. Coffman
THE COFFMAN LAW FIRM
First City Building
505 Orleans St., Ste. 505
Beaumont, TX 77701
Telephone: (409) 833-7700
Facsimile: (866) 835-8250
Email: rcoffman@coffmanlawfirm.com

Mitchell L. Burgess
BURGESS & LAMB, P.C.
1000 Broadway, Suite 400
Kansas City, MO 64105
Telephone: (816) 471-1700
Facsimile: (816) 471-1701
Email: mitch@burgessandlamb.com